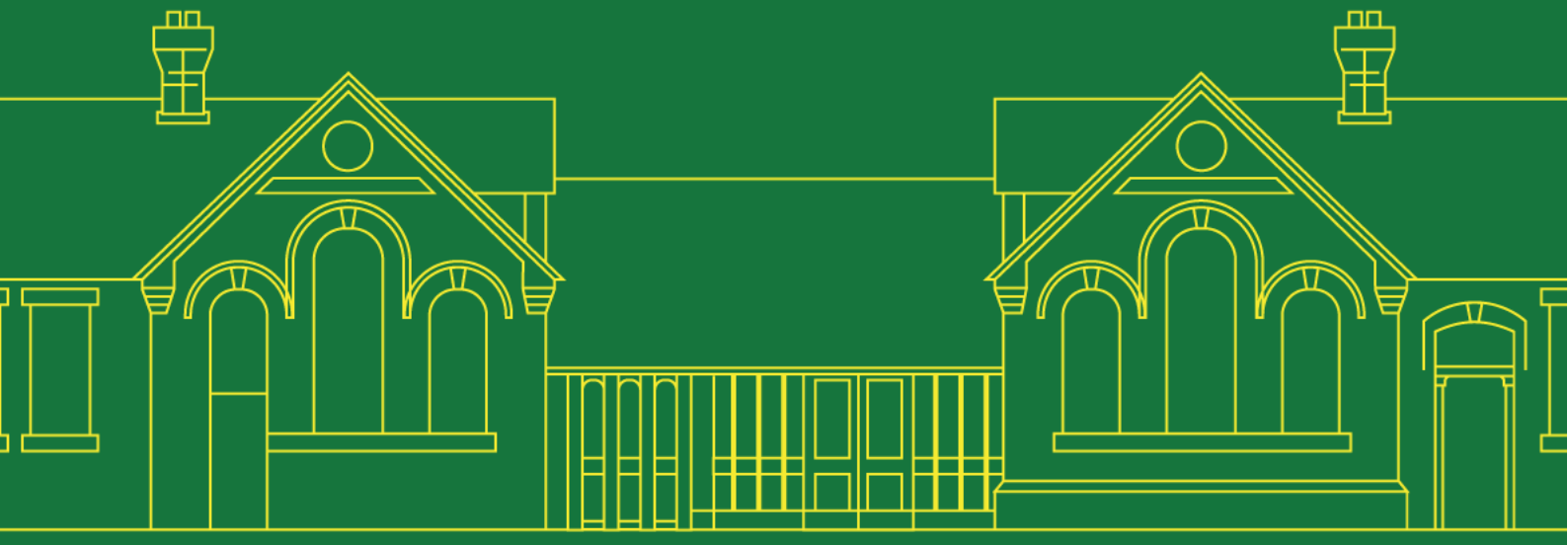
E-Safety Policy

September 2024



STOUR VALE ACADEMY TRUST

Queen Victoria Primary School Vision and Values

At Queen Victoria Primary School, we care deeply for the children of Sedgley; we believe every child is worthy and capable of success and happiness and this shows in every interaction. We create the conditions for children to grow into individuals who care about themselves, each other and the world they live in. We strive to make a positive difference by basing everything we do on our CARE principles:

Children are at the heart of everything we do - every day, in every decision, and every action, children's best interests and needs are put first. We have a team of compassionate staff who will move heaven and earth to ensure children get what they need to succeed.

Aspiration – We are full of hope, ambition, and the highest expectations for all children to have bright futures. Therefore, we are ambitious in the curriculum we offer and the standards we expect of ourselves.

Responsible – One of our key purposes is to help our children develop into respectful and responsible citizens who make positive contributions to life in Sedgley and beyond.

Excellence – We are relentless in our pursuit of providing excellence in education, with a balanced approach to academic achievement and personal development.

Scope of the E-Safety Policy

This policy applies to all members of the school community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other Online Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers regarding the searching for and of electronic devices and the deletion of data in the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

Roles and Responsibilities

The Governing Body

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).
All governors will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole school or college approach to safeguarding and related policies and/or procedures.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.
- Ensuring that the filtering and monitoring provision is reviewed and recorded, at least annually. (The review will be conducted by members of the SLT, the DSL, and the IT service provider and involve the responsible governor) - in-line with the DfE Filtering and Monitoring Standards

Headteacher and Senior Leaders

- The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.
- The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community

The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) deputies are set out in our child protection and safeguarding policy as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school child protection policy.

- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety.
- Liaising with other agencies and/or external services if necessary.
- Providing regular reports on online safety in school to the headteacher and/or governing board.
- This list is not intended to be exhaustive.

The Managed Service Provider

The managed service provider (RM), alongside the headteacher and DSL, are responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Conducting ongoing, full security checks and monitoring the school's ICT systems.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.
- Ensuring that any online safety incidents are logged (see appendix 5) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

The managed service provider is responsible for helping the school to ensure that it meets the Online safety/E-Safety technical requirements outlined by DGfL, which is aligned to national guidance. The managed service provides a number of tools to schools including Smoothwall monitoring and RM SafetyNet filtering.

CC4 Access and similar products, are applications that enable a user to remotely access documents and applications stored on the school/academy server/servers. The school/academy has responsibility for ensuring files and applications accessed via this system comply with information and data security practices.

The Curriculum Lead and Computing Coordinator

Curriculum Leads will work with the DSL/OSL to develop a planned and coordinated online safety education programme.
This will be provided through:

- PHSE and SRE programmes.
- Cross-curricular opportunities.
- assemblies and pastoral programmes.
- through relevant national initiatives and opportunities e.g. Safer Internet Day and Anti-bullying week.
- The computing curriculum.

All Teaching Staff, Support Staff and Volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy.
- Implementing this policy consistently.
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet and ensuring that pupils follow the school's terms on acceptable use.
- all digital communications with pupils / parents / carers should be on a professional level and only carried out using official school systems.
- Working with the DSL to ensure that any online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'.

This list is not intended to be exhaustive.

Parents and Carers

Parents/carers play a crucial role in ensuring their children understand the need to use the internet and devices in an appropriate way.
Parents are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy.
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet.
- Reinforce the online safety messages provided to children in school.

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

Educating Children About Online Safety

Pupils will be taught about online safety as part of the curriculum:
The text below is taken from the National Curriculum computing programmes of study.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.
All schools have to teach:

- Relationships education and health education in primary schools

In Key Stage 1, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in Key Stage 2 will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact
- By the end of primary school, pupils will know:
- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

Online safety is reinforced in all areas of the curriculum. Staff and volunteers should act as positive role models in their use of digital technologies, the internet and mobile devices.

Educating Parents About Online Safety

The school will provide information to parents and raise awareness of internet safety through:

- Newsletter, letters to families or other communications home
- our website and social media.
- Parent workshops
- Campaigns or events (such as Safer Internet Day)
- Parents' evenings and information/induction evenings
- Curriculum activities
- Signposting relevant information

We will inform parents about:

- The systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

This policy will also be shared with parents via the school website.
If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the headteacher and/or the DSL.
Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Education and Training for Staff

All staff members will receive training, including as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings). Advice/training will be provided to individuals as required.
By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.

- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
    - Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals.
Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

Education and Training for Governors

Governors take part in Online safety training or awareness sessions, including cyber security training. Online safety, including the school's filtering and monitoring duties, is covered through governor safeguarding training each year. Governors are also invited to attend school training sessions or parent workshops as appropriate.

Filtering and Monitoring

The school filtering and monitoring provision is agreed by senior leaders, governors and the Managed Service Provider. The DSL has lead responsibility for safeguarding and online safety, with support from the senior leaders and Managed Service Provider. Day-to-day management of the schools 'managed' infrastructure/network is delegated to the Managed Service Provider. They ensure the school system is as safe and secure as is reasonably possible.

Checks on the filtering and monitoring system are carried out by the Managed Service Provider with involvement of a senior leader.

Filtering

- The school manages access to content across its systems for all users and on all devices using the school's internet provision. The filtering provided meets the standards defined in the DfE Filtering standards for schools and colleges and the guidance provided in the UK Safer Internet Centre.
- Illegal content (e.g., child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation URL list and the police assessed list of unlawful terrorist content, produced on behalf of the Home Office. Content lists are regularly updated.
- There are established and effective routes for users to report inappropriate content, recognising that no system can be 100% effective.
- There is a clear process in place to deal with, and log, requests/approvals for filtering changes.
- Filtering logs are regularly reviewed and alert the senior leaders to breaches of the filtering policy, which are then acted upon.
- The school has provided enhanced/differentiated user-level filtering (allowing different filtering levels for staff and children)
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead and Online Safety Lead, or senior leaders; all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention.
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems using the appropriate blend of strategies informed by the school's risk assessment. These may include:

- Physical monitoring (adult supervision in the classroom)
- Internet use is logged, regularly monitored and reviewed.
- Filtering logs are regularly analysed, and breaches are reported to senior leaders.

- School technical staff regularly monitor and record the activity of users on the school technical systems, when appropriate.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- responsibility for technical security resides with SLT who may delegate activities to identified roles.
- all users have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the managed service provider and will be reviewed, at least annually, by the SLT.
- password policy and procedures are implemented.
- the security of their username and password and must not allow other users to access the systems using their log on details.
- all users have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details.
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone.
- the administrator passwords for school systems are kept in a secure place, e.g. school safe.
- there is a risk-based approach to the allocation of learner usernames and passwords.
- there will be regular reviews and audits of the safety and security of school technical systems.
- servers, wireless systems, and cabling are securely located and physical access restricted.
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, and devices from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up-to-date endpoint software.
- there are rigorous and verified back-up routines, including the keeping of network-separated (air-gapped) copies off-site or in the cloud,
- The managed service provider is responsible for ensuring that all software purchased by and used by the school is adequately licenced and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- personal use of any device on the school network is regulated by acceptable use statements that a user consents to when using the network.
- staff members are not permitted to install software on a school-owned devices without the consent of the SLT/IT service provider.
- removable media is not permitted unless approved by the SLT/IT service provider.

- systems are in place to control and protect personal data and data is encrypted at rest and in transit.
- mobile device security and management procedures are in place.
- guest users are provided with appropriate access to school systems based on an identified risk profile.

Mobile Devices

Mobile devices may be school owned/provided or personally owned and might include smartphones, tablets, notebooks, laptop or other technology that usually has capability of utilising the school's wireless network. The primary purpose of any use of mobile devices (either school-owned or personal) in school is educational. Any use of mobile devices should be done so in line with other school policies and procedures, including the safeguarding policy, behaviour policy, bullying policy, acceptable use policy and the staff code of conduct.

- The school Acceptable Use Agreements for staff, pupils and parents / carers will give consideration to the use of mobile technologies
- The school allows:

	School Devices		Personal Devices		
	School owned for single user	School owned for multiple users	Student owned	Staff owned	Visitor owned
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*			
Internet only				*Yes*	*Yes*
No network access			*Yes*		

School-owned devices

- Devices can be used in school to support teaching and learning and can also be taken out of school for work purposes.
- Personal use is not allowed.
- All devices have access to the school internet and are filtered by the school filtering system.

- The managed service provider is responsible for the management of devices, installation of apps and changing of settings and technical support. Devices are not regularly monitored but the school reserves the right to monitor as when they see feel it is needed. All staff have signed the Acceptable Use Policy.
- All devices in school are filtered by BT Lancashire Services (BTLS) systems.
- The devices have access to the teachers' one drive account and specific apps that use cloud storage.. These must be logged in by the teacher using the device.
- Devices are GDPR compliant through the use of passwords. These are school managed passwords.
- Taking photos and storing them on devices is allowed for school purposes (for example: evidencing work, blogging). Use of images must follow school policies concerning the sharing, distribution and publication of those images.
- If a teacher leaves the school, the device is given back and wiped so it can be used by a different member of staff.
- Devices are covered by school insurance for accidental damage, fire and theft. If it is lost by a member of staff then they will be responsible for replacing this.
- Staff are given appropriate training to use the devices and are familiar with all the relevant policies regarding use of devices.

Personal devices

- Staff and visitors are allowed to use personal mobile devices in school.
- Mobile phones may only be used in designated areas - in places in school where there are no children present (e.g. offices and the staffroom). Guests devices will be given access specific to the task / activity.
- Devices will not have access to the networks. Staff can have access to the internet, visitors are given access through a 'guest' login.
- No Technical support is available for personal devices.
- The school reserves the right to take, examine and search users' devices in the case of misuse (England only).
- Taking / storage / use of images of children in school is forbidden on personal devices.
- School takes no responsibility for the loss/damage or malfunction following access to the network. However, it is unlikely that any personal devices have access to the network.
- Access to the school internet is only given upon request.
- Pupils are educated about the safe and responsible use of mobile devices as part of Online Safety lessons.

Social Media

The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to learners through:

- ensuring that personal information is not published.
- education/training being provided including acceptable use, age restrictions, social media risks, digital and video images policy, checking of settings, data protection and reporting issues.
- clear reporting guidance, including responsibilities, procedures, and sanctions.
- risk assessment, including legal risk.
- guidance for learners, parents/carers

For official school social media accounts are established, there should be:

- a process for approval by senior leaders
- clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff.
- Consideration of the staff code of conduct
- systems for reporting and dealing with abuse and misuse.
- understanding of how incidents may be dealt with under school disciplinary procedures.

Where staff use social media professionally or personally:

Personal communications are those made via personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the school it must be made clear that the member of staff is not communicating on behalf of the school with an appropriate disclaimer. Such personal communications are within the scope of this policy.

- No reference should be made in social media to learners, parents/carers or school staff.
- Staff ensure they do not engage in online discussion on personal matters relating to members of the school community.
- Personal opinions should not be attributed to the school.
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.
- Staff act as positive role models in their use of social media
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

Monitoring of public social media

- As part of active social media engagement, the school may pro-actively monitor the Internet for public postings about the school.
- The school should effectively respond to social media comments made by others according to a defined policy or process.

- when parents/carers express concerns about the school on social media we will urge them to make direct contact with the school, in private, to resolve the matter. Where this cannot be resolved, parents/carers should be informed of the school complaints procedure.

Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. They should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website / social media / local press.
  We allow parents / carers to take videos or digital images of their children at school events for personal use. To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website, particularly in association with photographs.

Online Publishing

The school communicates with parents/carers and the wider community and promotes the school through:

- Public-facing website
- Social media
- Online newsletters

The school website is managed by The Headteacher. The school ensures that the online safety policy has been followed in the use of online publishing e.g., use of digital and video images, copyright, identification of young people, publication of school calendars and personal information – ensuring that there is least risk to members of the school community, through such publications.
Where learner work, images or videos are published, their identities are protected, and full names are not published.
The school website provides information about online safety e.g., publishing the school's Online Safety Policy and acceptable use agreements; curating latest advice and guidance; an online safety page with appropriate links.
The website includes an online reporting process for parents and the wider community to register issues and concerns to complement the internal reporting process.

Acceptable Use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school.
The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- communication with parents/carers
- being built into education sessions
- school website

User actions		Acceptable	Acceptable at certain ....times	Acceptable for Nominated Users	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Any illegal activity for example: • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences • Fraud and financial crime including money laundering					X
Users shall not undertake activities that might be classed as cybercrime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial/personal information, databases, computer/network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					X
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)				X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X		
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When using communication technologies, the school considers the following as good practice:

- When communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- Any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content. Personal e-mail addresses, text messaging or social media must not be used for these communications.
- Staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- Users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

Reporting and Responding to Incidents of Misuse

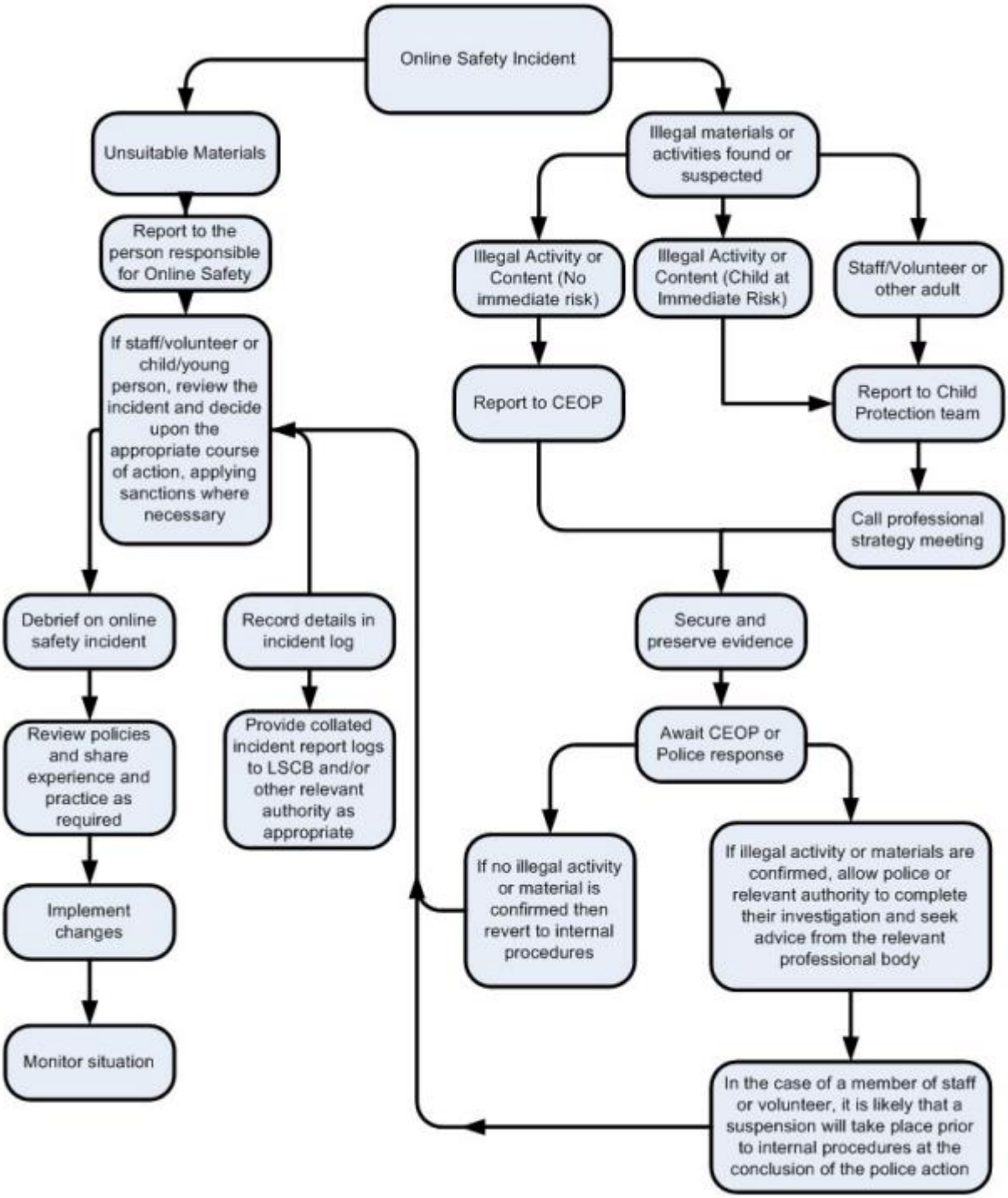
The school will take all reasonable precautions to ensure online safety for all school users but recognises that incidents may occur inside and outside of the school (with impact on the school) which will need intervention. The school will ensure:

- There are clear reporting routes which are understood and followed by all members of the school community which are consistent with the school safeguarding procedures, and with the whistleblowing, complaints and managing allegations policies.
- All members of the school community will be made aware of the need to report online safety issues/incidents.
- Reports will be dealt with as soon as is practically possible once they are received.
- The Designated Safeguarding Lead, Online Safety Lead and other responsible staff have appropriate skills and training to deal with online safety risks.
- If there is any suspicion that the incident involves any illegal activity or the potential for serious harm, the incident must be escalated through the agreed school safeguarding procedures, this may include:
    - Non-consensual images
    - Self-generated images
    - Terrorism/extremism
    - Hate crime/ Abuse
    - Fraud and extortion
    - Harassment/stalking
    - Child Sexual Abuse Material (CSAM)
    - Child Sexual Exploitation Grooming
    - Extreme Pornography
    - Sale of illegal materials/substances
    - Cyber or hacking offences under the Computer Misuse Act
    - Copyright theft or piracy

Any concern about staff misuse will be reported to the Headteacher, unless the concern involves the Headteacher, in which case the complaint is referred to the Chair of Governors and the CEO of Stour Vale Academy Trust. Where there is no suspected illegal activity, devices may be checked using the following procedures:

- One or more senior members of staff should be involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated device that will not be used by learners and, if necessary, can be taken off site by the police should the need arise (should illegal activity be subsequently suspected). Use the same device for the duration of the procedure.
- Ensure that the relevant staff have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed, and attached to the form.
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by local authority / MAT (as relevant)
    - Police involvement and/or action
- It is important that those reporting an online safety incident have confidence that the report will be treated seriously and dealt with effectively.
- There are support strategies in place e.g., peer support for those reporting or affected by an online safety incident.
- Incidents should be logged.
- Relevant staff are aware of external sources of support and guidance in dealing with online safety issues, e.g. local authority; police; Professionals Online Safety Helpline; Reporting Harmful Content; CEOP.
- Those involved in the incident will be provided with feedback about the outcome of the investigation and follow up actions.
- Learning from the incident (or pattern of incidents) will be provided to:
    - The Senior Leadership Team for consideration of updates to policies or education programmes and to review how effectively the report was dealt with.
    - staff, through regular briefings
    - learners, through assemblies/lessons
    - parents/carers, through newsletters, school social media, website
    - governors, through regular safeguarding updates
    - local authority/external agencies, as relevant

The school will make the flowchart below available to staff to support the decision-making process for dealing with online safety incidents.



School actions

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

Responding to Pupil Actions

	Refer to class teacher	Refer to AHT/DHT/DSL	Refer to Headteacher	Refer to police / social care	Refer to local authority technical support for advice or action	Inform parents/carers	Remove device/network access rights	Issue a warning	Further sanction in line with behaviour policy
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on User Actions on unsuitable/inappropriate activities).		X	X	X					
Attempting to access or accessing the school network, using another user's account (staff or learner) or allowing others to access school network by sharing username and passwords	X	X	X						
Corrupting or destroying the data of other users.	X	X	X					X	
Sending an e-mail, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X			X		X	
Unauthorised downloading or uploading of files or use of file sharing.	X	X	X						
Using proxy sites or other means to subvert the school's filtering system.	X	X	X			X		X	
Accidentally accessing offensive or pornographic material and failing to report the incident.	X	X	X			X			
Deliberately accessing or trying to access offensive or pornographic material.	X	X	X			X		X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act.	X	X	X			X			
Unauthorised use of digital devices (including taking images)	X								

Unauthorised use of online services	X								
Actions which could bring the school into disrepute or breach the integrity or the ethos of the school.	X	X	X			X			
Continued infringements of the above, following previous warnings or sanctions.	X	X	X			X	X		X

Responding to Staff Actions

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.
The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy
- Behaviour policy
- Staff Code of Conduct
- Data protection policy and privacy notices
- Complaints procedure

GDPR Personal Data

This policy adheres to the principles under data protection law. For further information please review the school's data protection policy published on the school's website.

E-Safety/Online Safety Tools available on the DGfL Network

E-Safety tool	Type	Availability	Where	Details
Smoothwall filtering	Web filtering	Provided as part of DGfL	All network connected devices within DGfL	Gives schools the ability to audit, filter and un-filter websites
RM Tutor	Teacher support	Provided as part of DGfL	Managed school desktops	Allows teachers to view and demonstrate screens, control hardware and distribute work
CC4 AUA	Awareness raising	Part of CC4- needs to be enabled	All CC4 stations at log in	When enabled through the management console, users are given an acceptable use policy at log in
eSafe	Monitoring software- *licenses available on Windows, Apple Mac*	Available to all schools	All school desktops and networked laptops, Chrome books and Apple Mac networks	Takes a snapshot of a screen when an event is triggered. A range of events can be monitored. Reports are sent to designated staff in school
Email	Filtering and list control	Provided as part of DGfL	Office 365	Allows schools to restrict where email is sent from/to
DGfL 'Security Enhancements'	Safe practice	Provided as part of DGfL3	All CC4 stations	A password management policy that enforces password rules of complexity and length for different users

Staff/Volunteer Acceptable Use Agreements are intended to ensure that:

- staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- staff are protected from potential risk in their use of technology in their everyday work

Pupil Acceptable Use Agreements are intended to ensure that:

- young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use
- school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students/pupils* to agree to be responsible users

When forming a pupil AUA, you may want to consider statements that focus on:

- For my own personal safety
- Understanding that everyone has equal rights to use technology as a resource
- Acting as I expect others to act toward me
- Understanding that I am responsible for my actions both inside and outside of the educational establishment

Best practice indicates that pupils involved in formulating AUA's have a greater awareness of the importance of adhering to the agreed principles.

Community Users Acceptable Use Agreements are intended to ensure that:

- community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- users are protected from potential risk in their use of these systems and devices

Primary Pupil AUA for KS1 and electronically

Queen Victoria Primary School –

Acceptable Use Agreement (AUA for Children

When I log on I agree that:

I will only use my own username and password to log on. I will keep my password secret.

I will only use websites that have been suggested by the teacher or a grown up.

I will not give out personal information; tell people where I live, my phone number or where I go to school without permission from the teacher/parent.

I will always ask an adult before sharing photos. I will only share photos that I don't mind everyone seeing.

I will tell a grown up if I feel scared or unhappy about anything I find when using the school computers/laptops.

I will respect school property; I will use the internet, computers and laptops and all other equipment properly.

Primary Pupil AUA

Queen Victoria Primary School –

Rules for Responsible Internet Use for Primary Pupils

The school has installed computers and provided Internet access to help our learning. I understand that the school may check my computer files and may monitor any Internet sites I visit.

These rules will keep everyone safe and help us to be fair to others. It is important that you read this policy carefully. If there is anything that you do not understand, please ask.

I agree that:

I will not share any of my passwords with anyone, or use another person's password. If I find out someone else's password, I will tell that person and a member of the school staff, so they can change it.

I will use a password which contains some small and some big (capital) letters plus a number or a symbol *e.g. Skool5 or com**2er* and change it on a regular basis.

I will use the technology at school for learning. I will use the equipment properly and not interfere, change or delete someone else's work.

If I use a flash drive or other storage device, I will follow school guidelines on their use.

I will only e-mail people I know, or my teacher has approved.

If I attach a file to an email, it will not include any inappropriate materials (something I would not want my teacher to see or read) or anything that threatens the integrity of the school ICT system.

I will be respectful in how I talk to and work with others online and never write or participate in online bullying. If anyone sends me a message, I do not like or feel uncomfortable about I will show it to my teacher or parent.

I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other pupils and myself.

I will not download any programmes or games on to the school computers, netbooks or laptops unless I have permission to do so.

I will always check with a responsible adult before I share or publish images of myself, my friends or other people onto the internet.

I will not make audio or video recordings of another pupil or teacher without their permission.

When using sites on the internet, I will not give my name, home address, telephone/mobile number, pretend to be someone else or arrange to meet someone I do not know, unless my parent, carer or teacher has given permission.

I will always follow the 'terms and conditions' when using a site. The content on the web is someone's property and I will ask my teacher to help me get permission if I want to use information, pictures, video, music or sound files.

I will think carefully about what I read on the Internet, question if it is from a reliable source and use the information to help me answer any questions (I should not copy and paste the information and say it's my own work).

If I want to connect my own device to the school network, I will check with my teacher to see if it is possible.

I am aware of the CEOP report button and know when to use it.

I know anything I do on the computer may be seen by someone else.

Signed: .....

PRINT NAME: .....

Dated: .....

Staff AUA

Queen Victoria Primary School –
Staff Acceptable Use Agreement
Rules for Responsible Internet Use

The computer systems within the Trust/School are made available to students, staff and other adults to further their education and to enhance professional activities including teaching, research, administration and management. The Trust's Acceptable Use Policies have been drawn up to protect all parties – the students, the staff, other adults and the Trust, and are reviewed on a regular basis. Staff and other adults working within the school who wish to use the Trust's computer systems, email or internet should sign a copy of this Acceptable Use Statement.

- All internet activity should be appropriate to the student's education.
- Access should only be made via the authorised account and password, which should not be made available to any other person.
- Activity that threatens the integrity of the Trust's ICT systems or activity that attacks or corrupts other systems is forbidden.
- Users are responsible for all email sent and for contacts made that may result in email being received.
- Use for personal financial gain, gambling, political purpose or advertising is forbidden.
- Copyright of materials must be respected.
- Posting anonymous messages and forwarding chain letters is forbidden.
- As emails can be forwarded or inadvertently be sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media.
- Use of the network to access inappropriate materials such as pornographic, racist or other offensive material is forbidden.
- If you access any site on the internet which you feel is inappropriate, report it in writing as soon as possible. Retain a copy of the report and return the pro-forma to the identified member of staff.

Misuses of the Trust's computer equipment, email or the internet are serious offences. School may monitor the use of the email and internet services provided as part of their network management; this information may be recorded and may be used in disciplinary procedures if necessary. The School and Stour Vale Academy Trust reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or government request.

Acceptable Use Agreement

I have read the above statement and agree to abide by the conditions. I understand that misuse of the Trust's computer systems, email or the internet are serious offences and could lead to disciplinary procedures, up to an including dismissal.

Signed:	
Print Full Name:	
Date	

Community

Queen Victoria Primary School –
Community User – Acceptable Use Policy
Rules for Responsible Internet Use

This policy applies to all community users of the school's systems, who have guest access to the internet. We trust you to use the ICT facilities sensibly, professionally, lawfully, and in accordance with this Policy.

It is important that you read this policy carefully. If there is anything that you do not understand, please ask. Once you have read and understood this policy thoroughly, you should sign this document, retain a copy for your own records and return the original to the school office.

Research Machines (RM) has a contractual obligation to monitor the use of the internet and e-mail services provided as part of DGfL, in line with The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. Traffic data and usage information may be recorded and RM, Dudley MBC and the school reserve the right to disclose any information they deem necessary to satisfy any applicable law, regulation, legal process or governmental request.

When entering an internet site, always read and comply with the terms and conditions governing its use. Be aware at all times that when visiting an internet site, the unique address for the computer you are using (the IP address) can be logged by the site you visit, thus identifying our school. For your information, the following activities are criminal offences under the Computer Misuse Act 1990:

- unauthorised access to computer material i.e. hacking;
- unauthorised modification of computer material; and
- unauthorised access with intent to commit/facilitate the commission of further offences.

In line with this policy, the following statements apply: -

- Do not download any image, text or material which is copyright protected without the appropriate authorisation.
- Do not download any image, text or material which is inappropriate or likely to cause offence. If this happens accidentally report it to a member of staff
- If you want to download any software, first seek permission from the member of staff responsible. They should check that the source is safe and appropriately licensed.

- You should not:
    - introduce packet-sniffing software (i.e. software which is used to intercept data on a network) or password detecting software;
    - seek to gain access to restricted areas of the network;
    - knowingly seek to access data which you are not authorised to view;
    - introduce any form of computer viruses;

I have read through and fully understand the terms of the policy. I also understand that the school may amend this policy from time to time and that I will be issued with an amended copy.

Signed: .....

PRINT NAME .....

Dated: .....

Staff Guardianship Loan Form

Queen Victoria Primary School –
Portable ICT Equipment – Staff Guardianship Loan Form

Name ..... has permission to loan and is guardian of the following item(s) of ICT equipment: -

Item	Serial No	Start date	Return date

Whilst the above items are in your care, the school will expect you to take full personal responsibility for the safe custody of all of the items listed and to follow the guidelines below: -

- I will ensure the mobile device is secured or locked away when not in use;
- I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives/memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure the Anti-virus- software, where appropriate, is kept up to date;
- I will ensure that data remains confidential and secure;
- Where personal data about staff or pupils, or school confidential data, is stored on the device, the device will be encrypted and password protected (as appropriate to the device), and the data will be removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Signed ..... Date .....

Name person authorising the loan .....

Signed ..... Date .....

Pupil Guardianship Loan Form

Queen Victoria Primary School –
Portable ICT Equipment – Pupil Guardianship Loan Form

Name ..... has permission to loan and is guardian of the following item(s) of ICT equipment: -

Item	Serial No	Start date	Return date

Whilst the above item is in your care, the school will expect you to take full personal responsibility for the safe custody of this item and to follow the guidelines below: -

- I will look after the device. I will ensure it is secured or locked away when not in use;
- I agree to use it sensibly. I will ensure that unauthorised software is not loaded or run on this mobile device;
- I will not download, store or collect any inappropriate material on the device
- I will ensure that all external media sources (discs, USB flash drives/memory sticks) are checked for viruses before data transfer to the mobile device where appropriate;
- I will ensure the device is regularly virus-checked where appropriate;
- I will ensure that data remains confidential and secure;
- Any personal data stored on the device will be encrypted if appropriate and removed as soon as reasonably possible
- I will ensure that the equipment is not used by anyone who has not been authorised by the school
- I will return the device upon request and when I am on leave or other absence, unless otherwise authorised.
- I will ensure the equipment is not left unattended in any vehicle (as this is not covered by the school's insurance policy), and accept that any loss arising from a loss from a vehicle will be my own responsibility.
- If the equipment is lost or stolen, I will inform the police as soon as possible to get a crime number and also contact the appropriate member of staff

Parents' Consent Form

I give permission for my son/daughter ..... (Name)
to receive a ..... for the duration of the project.
Signed ..... (Parent/Carer)

Name person authorising the loan .....

Signed ..... Date .....